

Foundational and Systems Support for Quantitative Trust Management (QTM)

Insup Lee (PI)

Computer and Information Science
University of Pennsylvania

ONR MURI N00014-07-1-0907
Review Meeting
November 4, 2009

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 04 NOV 2009		2. REPORT TYPE		3. DATES COVERED 00-00-2009 to 00-00-2009	
4. TITLE AND SUBTITLE Foundational and Systems Support for Quantitative Trust Management (QTM)				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Pennsylvania, Computer and Information Science, Philadelphia, PA, 19104				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES ONR MURI Review, Nov 2009.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 22	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Project Team

Principal Investigators

- **Sampath Kannan** (Ph.D 89, Berkeley)
Stream Algorithms, Run-time monitoring, Cryptography
- **Insup Lee** (Ph.D. 83, Wisconsin)
Real-time and cyber-physical systems, Run-time monitoring
- **Matt Blaze** (Ph.D. 93, Princeton)
Network security, Cryptography, Trust Management
- **Oleg Sokolsky** (Ph.D. 96, SUNY-SB)
Formal methods, Real-time and hybrid systems
- **Jonathan Smith** (Ph.D. 89, Columbia)
Networking, Security and privacy, Mobility
- **Angelos Keromytis** (Ph.D. 01, Penn)
Computer security, Cryptography, Networking
- **Wenke Lee** (Ph.D. 99, Columbia)
System and network security, Applied cryptography, Data mining

Students

- Adam Aviv, Jian Chang, Nikhil Dinesh, Zhiyi Huang, Andrew West, David Dagon, Manos Antonakakis, Matt Burnside, Vasilis Pappas, Stelios Sidiroglou

Postdocs

- Daniel Luo, Vinayak Prabhu, Krishna Venkatasubramanian,

Collaborators

- Nick Feamster, Boon Loo, Aravind Joshi, Jason Nieh

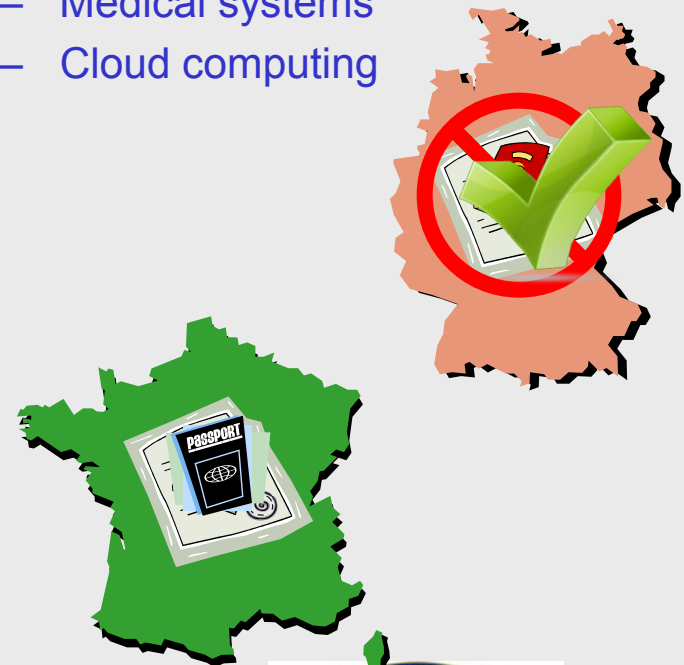


Trust

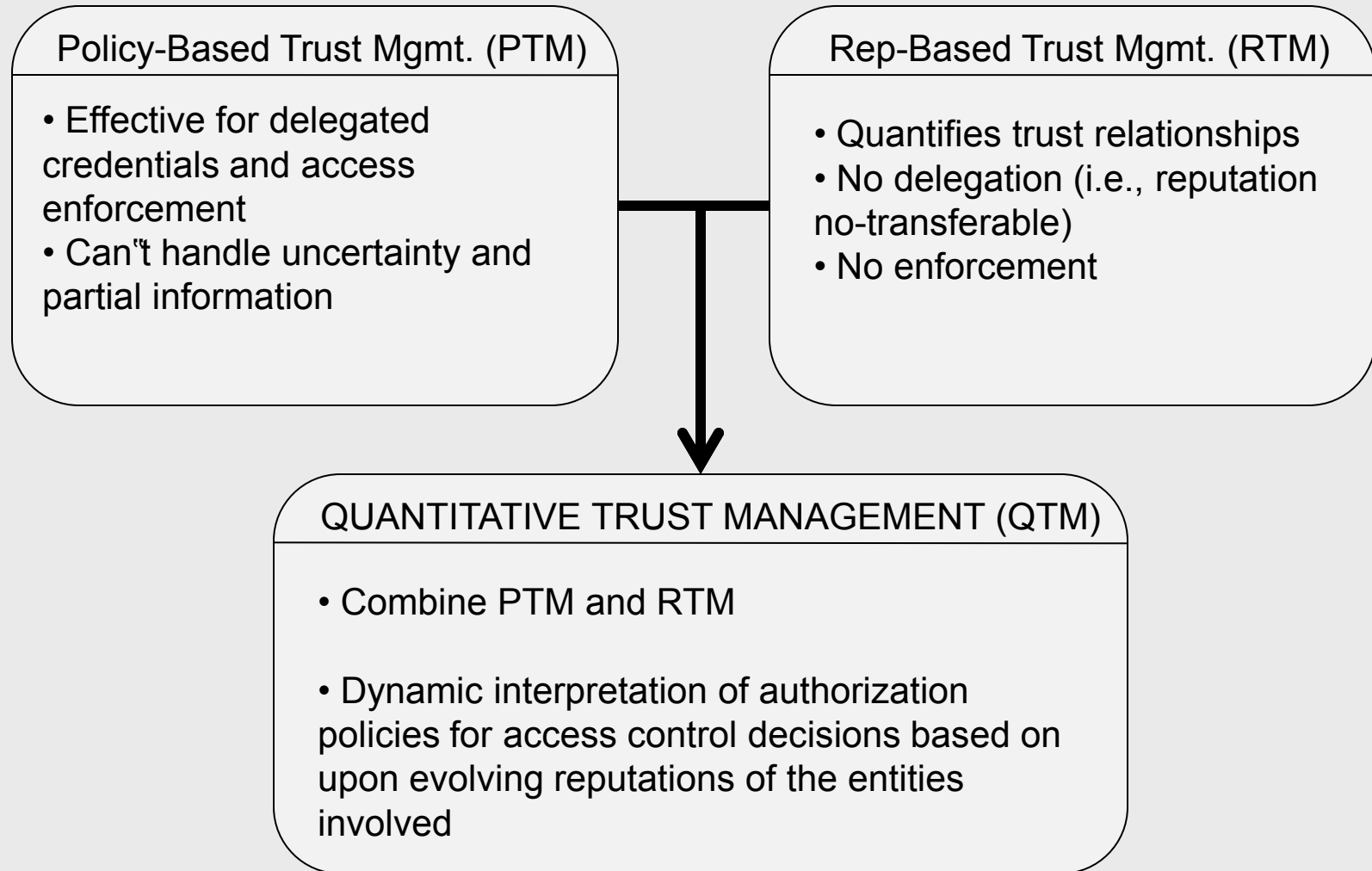
- Webster's Dictionary: TRUST, -noun:
 - (1) Assured reliance on the character, ability, strength, or truth of someone or something.
 - (2) One in which confidence is placed.
- Our Definition:
 - Trust is the expectation of a **trustor** with respect to certain properties of a **trustee** or her actions under a specified **context** and **time**, considering the **risks**, **incentives**, and **historical information**.

The Problem of Trust

- *Quantitative Trust* for federated networked systems
 - Decentralized policies
 - Dynamic environment, partial trust
 - Complex “trust” models (logic + reputation), in reality
- Applications
 - E-commerce systems
 - Service compositions in GIG
 - Reusing components/subsystem in complex DoD systems
 - Social Networks
 - Medical systems
 - Cloud computing



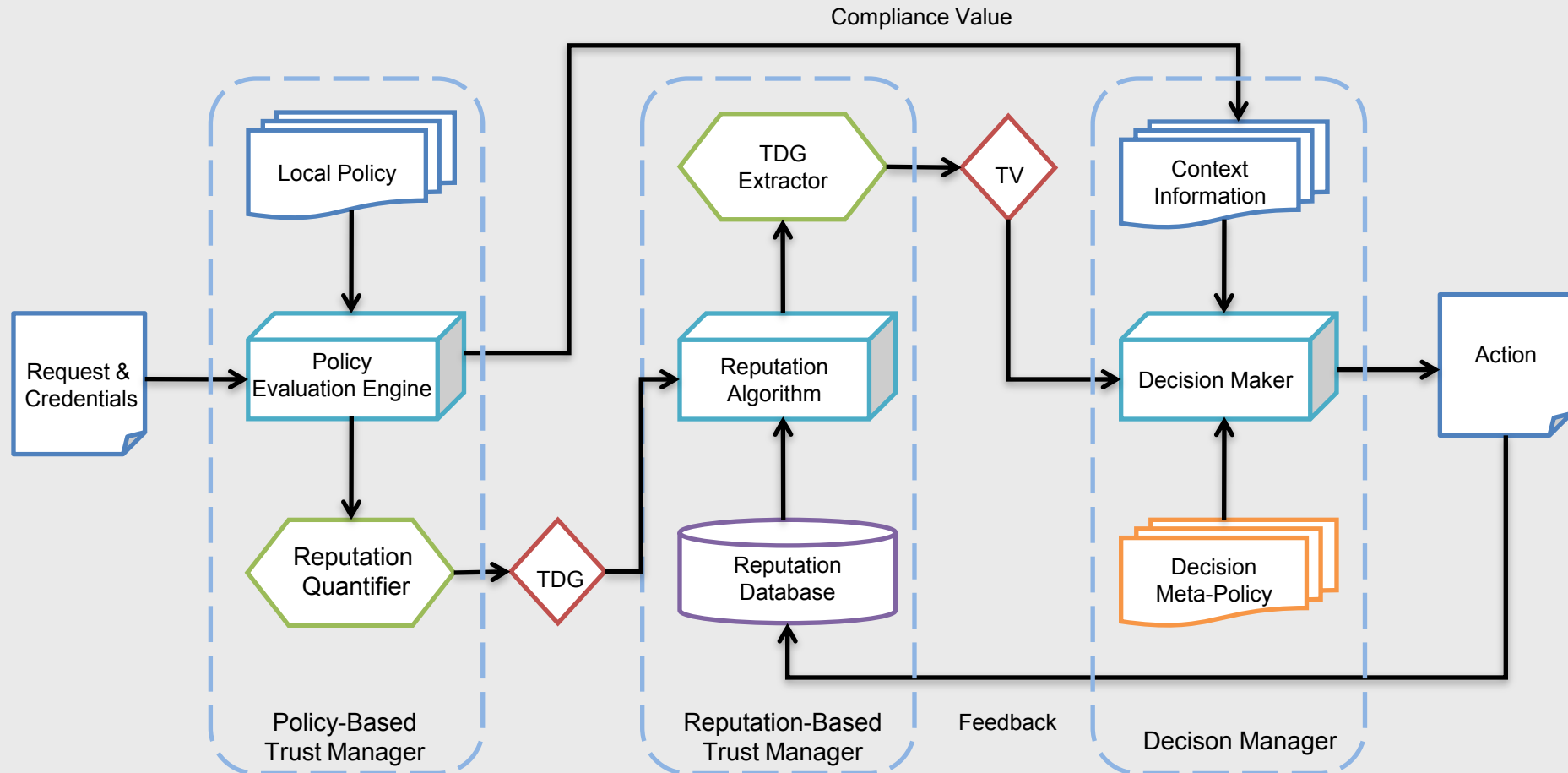
Trust Management



QTM Challenges

- What are some metrics for effectiveness of TM systems?
- How do we incorporate uncertainty in policy-based TM"s?
- How do we incorporate dynamism in policy-based TM"s?
- How can we model adversaries as **economic agents** and develop a **game-theoretic view** of trust management?
- Can we build new reputation management systems based on sound principles?
- What is the proper way to mathematically **combine reputations**?
 - Involves integration of logical/quantitative/probabilistic reasoning
 - Is there a means to build consensus from distributed observations?
- How do we **integrate** policy-based and reputation-based TMs?
- What are some important applications of TM systems?

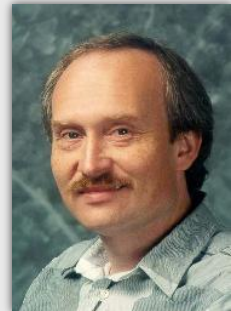
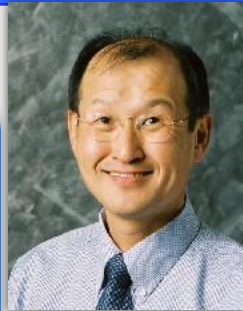
Quantitative Trust Management (QTM)



Collaboration



Policy-based Trust Management (PTM)

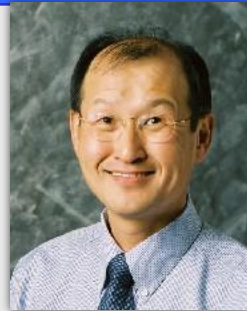


KeyNote PTM Systems

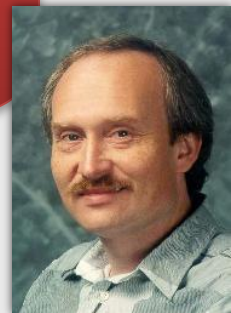
Permission-to-Speak

Dynamic Trust Management
Arachne

Collaboration



Reputation-based Trust Management (RTM)

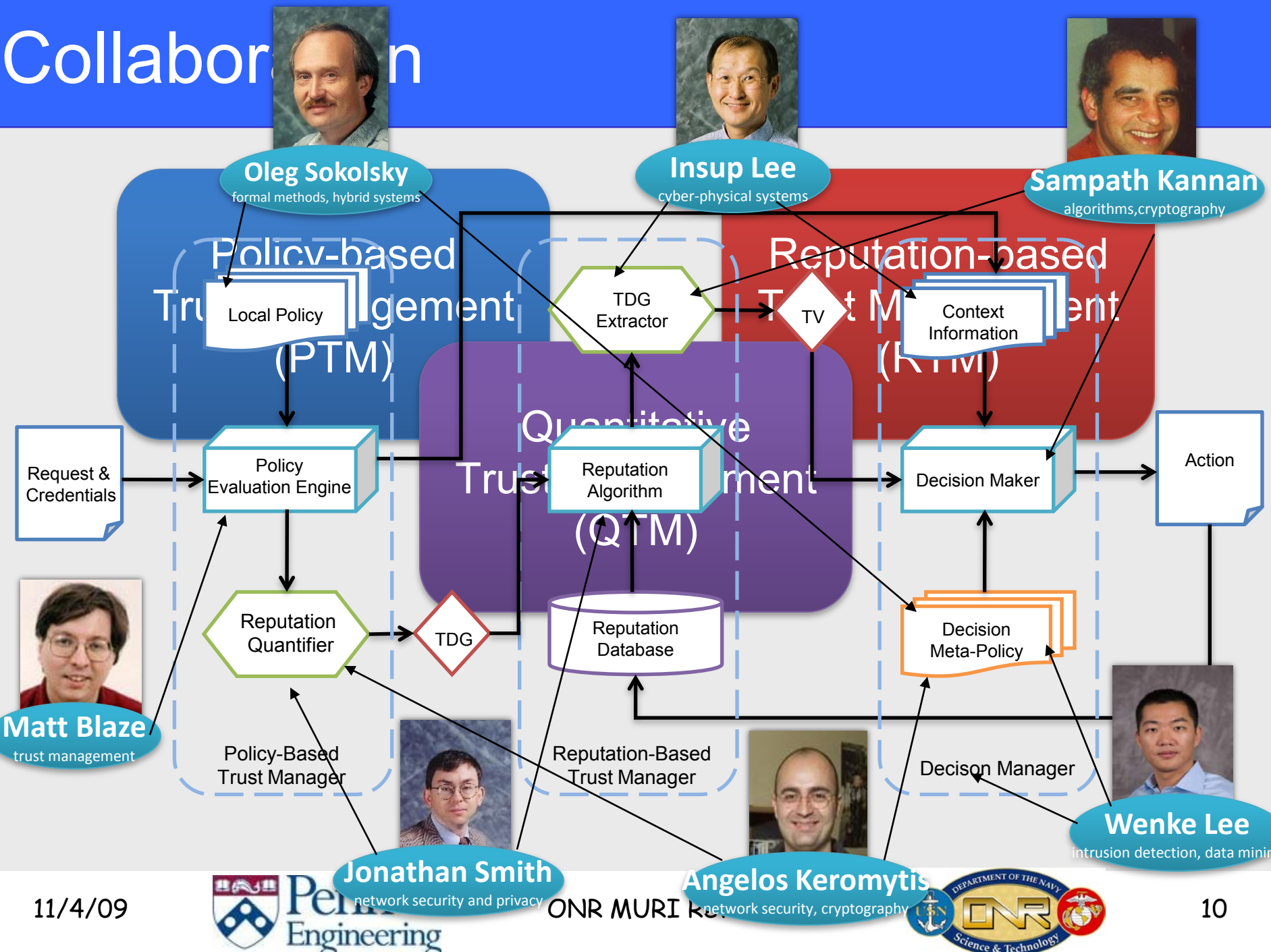


Evaluating RTM Systems

Blacklist as Feedback of
Reputation Management



Collaboration



Team Efforts

- Several Research Collaborations
 - Distributed TM, Dynamic TM, Spatio-Temporal Reputations, ...
 - Keynote-base QTM
- Annual meetings
 - 2007, 2008, 2009
- Many Tele-conferences and Student Visits
 - Penn -> GA Tech, Columbia -> Penn, GA Tech -> Penn
- Collaborative case studies
 - SPAM list and BGP security as QTM application
- PhD Dissertation Committees
 - Matt Burnside (Columbia)
 - David Dagon (GA Tech)
 - Andrew West (Penn)

Education

- Courses
 - Integrated material into COMS W4180 course (Columbia)
 - CIS 125 new course on understanding of existing and emerging technologies, along with the political, societal and economic impacts of those technologies (Penn)
 - Integrated material into CIS 551 (Penn)
 - Material on botnet detection added to Network Security classes: undergraduate cs4237, and graduate cs6262 (GA Tech)
 - 3 senior design projects (Penn)
- Workforce training
 - 3 post-docs
 - 10 Ph.D. students
 - 1 Masters and 1 undergraduate

Publication

- Publications
 - 7 journal articles
 - 2 book chapter
 - 33 conference papers
- Selected papers
 - M. Blaze, S. Kannan, I. Lee, O. Sokolsky, J.M. Smith, A.D. Keromytis, and W. Lee. Dynamic Trust Management, In IEEE Computer Magazine, vol. 42, no. 2, pp. 44 - 52, February 2009.
 - A.G. West, A.J. Aviv, J. Chang, V. Prabhu, M. Blaze, S. Kannan, I. Lee, J.M. Smith, and O. Sokolsky. QuanTM: A Quantitative Trust Management System. EUROSEC 2009, pp. 28-35.
 - A.G. West, I. Lee, S. Kannan, and O. Sokolsky. An Evaluation Framework for Reputation Management Systems. In *Trust Modeling and Management in Digital Environments: From Social Concept to System Development* (Zheng Yan, ed.), 2009.

Dissemination & Tech transfer

- Beyond conference talks
 - 7 invited and 2 keynote talks, 6 panels
- Working with Symantec to determine modus operandi of rogue Antivirus sites (and why users trust them)
 - Interim Symantec Threat Report (ISTR), Oct 09
- Working with Damballa to deliver botnet detection and mitigation technologies to government and enterprise customers
 - Botnet detection system such BotMiner malware analysis technologies, and the DNS-based monitoring technologies
 - Several Ph.D. students did summer internship
 - Several Damballa researchers were former students at Georgia Tech, and still participate in some of the research meetings at Georgia Tech
- Matt Burnside now working for NSA
- QTM ideas used in ONR-supported "Networks Opposing Botnets" (NoBot) project, with Penn, Harvard and Princeton

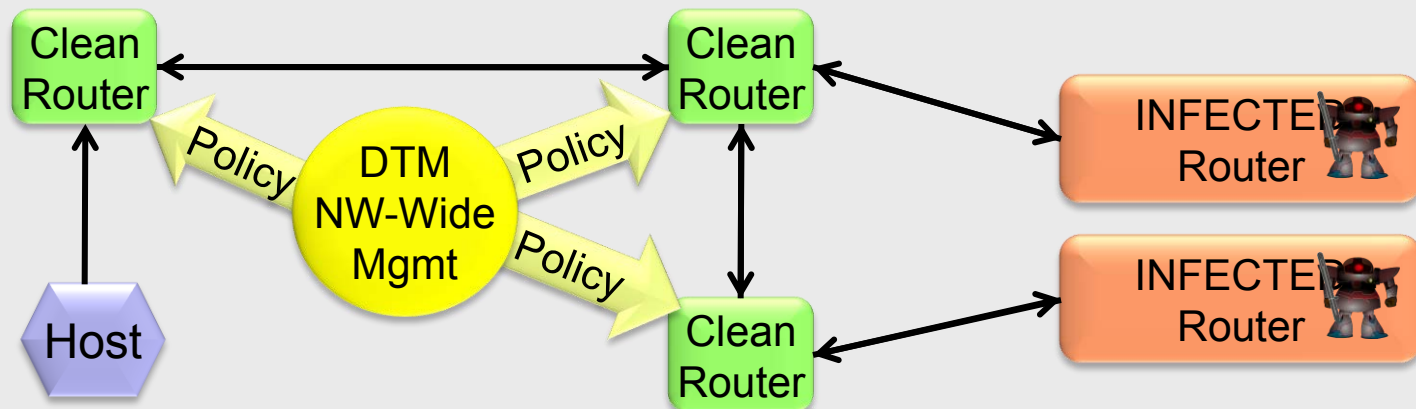
Research highlights

- Project Overview, Insup Lee (PI)
- Trust Management, Matt Blaze
- Dynamic Trust Management, Jonathan M. Smith
- Exposing Trust Assumptions in Distributed Policy Enforcement, Angelos Keromytis
- Permission to Speak: A Novel Formal Foundation for Access Control, Oleg Sokolsky
- Dynamic IP Reputation from DNS, Wenke Lee
- Using Spatiotemporal Reputation to Predict Malicious Behaviors, Andrew West
- Reputations and Games, Sampath Kannan
- Future Work and Discussion, Insup Lee

Dynamic Trust Management

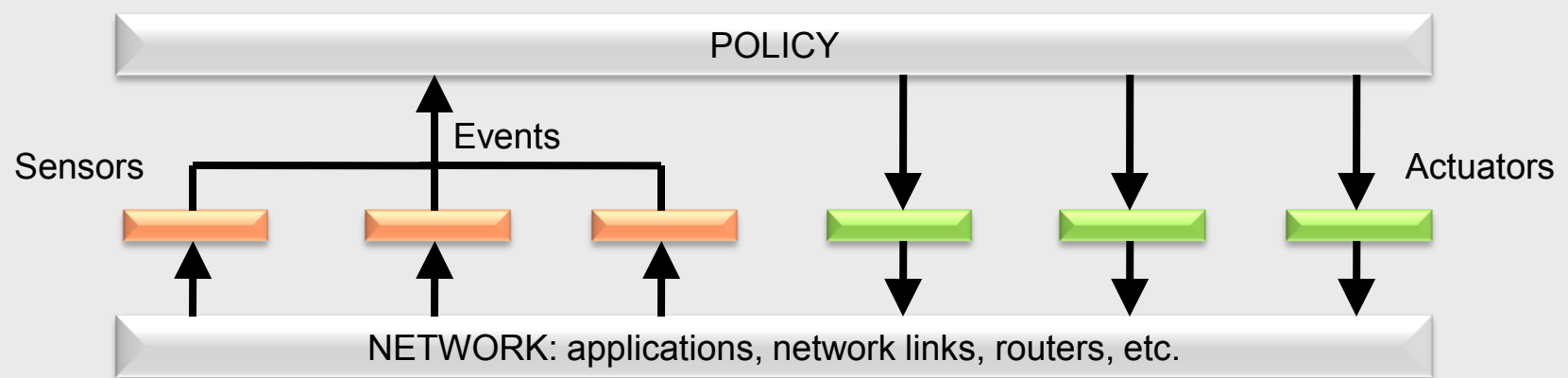
(Penn + Columbia + Georgia Tech)

- A **COOPERATIVE** and **DYNAMIC** policy evaluation infrastructure that will enable such critical capabilities as:
 - Adaptation to dynamic service availability
 - Complex situational dynamics (e.g., differentiating between bot-net and physical attacks on infrastructure).
- **BENEFITS** of a Dynamic Trust Management approach
 - Flexible and robust control of authorizations in complex distributed systems such as the DoD/IC GIG
 - The ability to define policies for scalable decentralized defense against emergent cyber-threats by rapid adaptation of resource access limits.



Arachne: Coordinated Policy Enforcement

(Columbia)



- **ARACHNE** is a system for the coordinated distribution and evaluation of a system-wide policy on different nodes
 - Several prototype systems for enterprise-level security have been developed
- **GOAL:** Integrate a variety of different, diverse security mechanisms and policy expression methods
 - Achieve enhanced protection over any individual method
 - Allow exchange of information between different mechanisms (Eliminate the possibility of “locally correct” but globally wrong decisions)
 - Capture trade-offs between amount of global context, scalability, etc.

Permission-to-Speak

- A new policy deontic logic developed under ONR-MURI
- Explicit representation of **PERMISSIONS** and **OBLIGATIONS** imposed by a policy, and the delegation of policies.
 - Captures notions such as „allow to require“ which are necessary for dynamic policy introduction.
- Explicit representation of policy **DEPENDENCIES**
 - Iterative algorithm for calculating the set of relevant policy statements
- Logic prog.-based evaluation allows efficient blame assignment

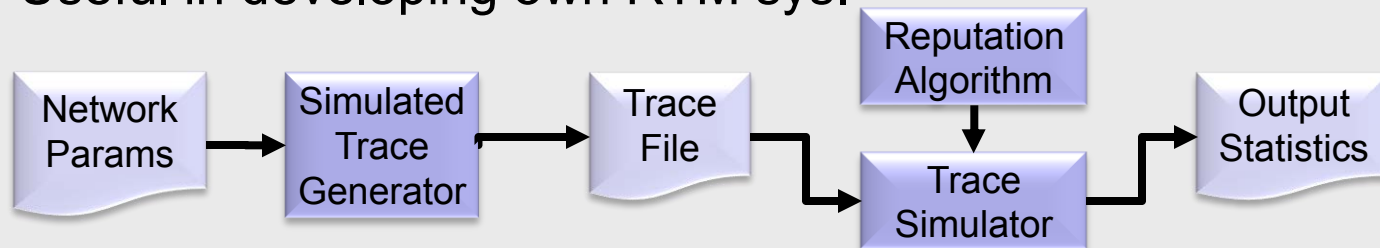
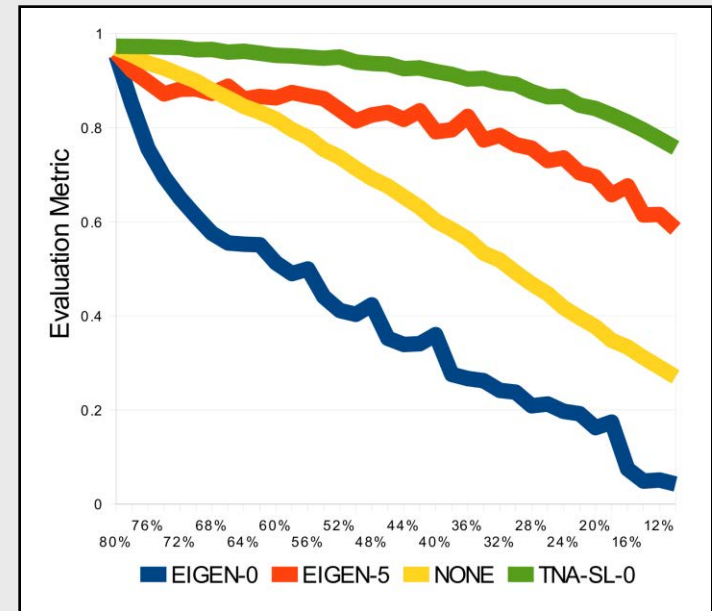
P_{pat} says_{pat} O_{hosp} says_{hosp} P_{pat} access(pat, record(pat))



Patients are allowed to ask a hospital for their medical records. In response, the hospital must permit access.

Evaluating RTM Systems

- Many reputation systems are available in the literature
 - EigenTrust, TNA-SL (Trusted Network Analysis with Subjective Logic), ...
 - Little or no comparison between them
- Designed and implemented a framework for comparative evaluation of reputation systems
 - Identified evaluation criteria
 - Generation of evaluation scenarios
 - Development of malicious strategies
 - Collection of statistics and analysis
- Useful in developing own RTM sys.



Dynamic IP Reputation from DNS

(Georgia Tech)

- Dynamic Domain Name reputation using passive DNS (pDNS)
 - Professional DNS hosting differs from non-professional
 - pDNS information is already present in our network
 - Static IP/DNS blacklists have limitations
 - Malicious Users tend to reuse their infrastructure
- Contributions:
 - Zone and network based clustering of pDNS
 - A new method of assigning reputation on new RRSETs using limited {White/Grey/Black}-listing
 - A dynamic Domain Name reputation rating system
 - Always maintain fresh reputation knowledge based on pDNS

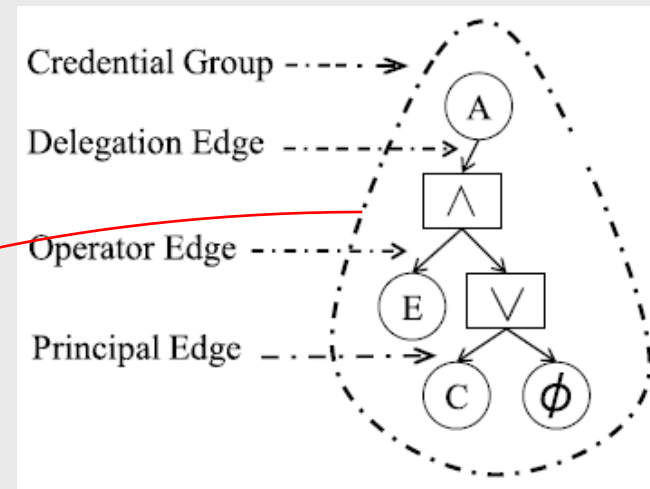
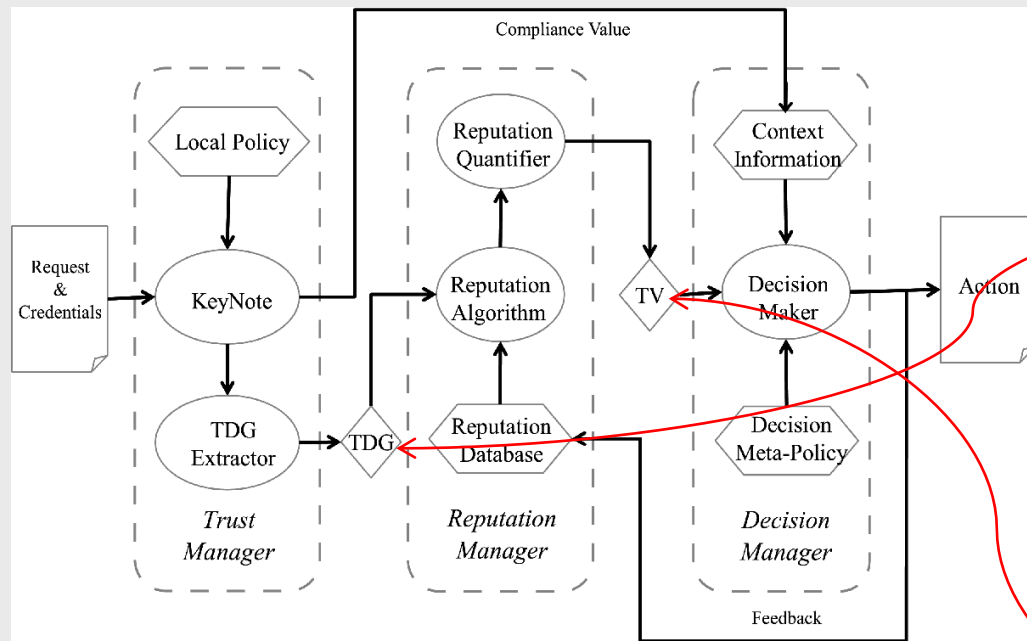
Spatio-Temporal Reputation

(Penn + Georgia Tech)

- As the RM part of QTM, we have developed reputation-bases trust management based on spatiotemporal reputation
- Approach
 - Assumptions
 - Bad guys are geographically clustered (spatio)
 - Bad guys are likely to repeat bad behaviors (temporal)
 - Given
 - A historical record of those principals known to be bad, and the time when this was noted (feedback)
 - Produce
 - An extended list of principals who are thought to be bad at the current time, based on their own past history, and the history of those around them
- Case studies: Spam filter based on IP blacklist, wikipedia

Quantitative Trust Management (QTM)

- QTM provides a dynamic interpretation of authorization policies for access control decisions using evolving reputations of parties
- QuanTM* is a QTM system that combines elements from PTM and RTM to create a novel method for trust evaluation



Trust Dependency Graph (TDG),
encoding PTM relationships
useful for RTM

Reputations of PRINCIPALS,
DELEGATIONS and
CREDENTIALS are
aggregated

The QuanTM Architecture